REMARKS

Applicants would first like to express their appreciation to Examiner Daniel L. Hoang for this examination.

Claims 1-14 are pending in the present application and each stand rejected under 35 U.S.C. 102 as being anticipated by U.S. Patent No. 6,317,868 to Grimm et al., hereafter Grimm.

Applicants respectfully contend that claim 1, 8, and 14, as originally filed are allowable because they include a feature that is neither disclosed nor suggested by Grimm or any other references cited in the Office Action, either individually or in combination, namely, "in response to a system call, executing a hook routine at a location of said system call," or "responsive to a system call for executing , executing a hook routine at a location of said system call." As described in the present application, in an exemplary embodiment a system call is an operation which transfers control of a processor, such as by stopping the current processing in order to request a service provided by an interrupt handler. The interrupt handler in turn is a program code at a memory location identified by an interrupt vector table. In this example, when a program makes a system call, the system call comprises an interrupt. By use of the interrupt vector table, the system executes the software routine located at the memory location designated (or pointed to) for the particular interrupt in the interrupt vector table. In claim 1, when a program makes a system call during execution of the program, the processor is pointed to a memory location for the system call. This is significant because the programming level at which software interrupts work is the level at which many computer viruses work (see specification page 8, line 30 to page 9, line 1). Moreover, the present application clearly indicates that it is desirable to hook the lowest level calls where possible (see specification page 9, lines 4-5).

Grimm does not disclose or suggest responding to a system call. Rather, Grimm provides for intercepting a software component when a component system (i.e., a computer or workstation issues a command to load the software. Thus, Grimm responds to a command to load a software component and not to a system call during execution of a program. Grimm does not operate at the programming level at which many computer viruses work. Instead, Grimm modifies a software component prior to execution to conform to security policy.

Also, Grimm does not disclose or suggest executing a hook routine. In the present invention, the hook routine is a program that works at the transfer of control of a processor. Instead, Grimm provides that a new software component (and not the processor) is intercepted. The new software component is then modified prior to execution. Grimm provides that "original" software be intercepted in response to a component system command to load the "original" software. Grimm provides intercepting software, while executing a hook routine does not intercept software, but rather transfers control of a processor. Grim does not disclose or suggest control of processing, but control of the software component. Moreover, Grimm is ambiguous as

to how the software is intercepted.

Nor does Grimm disclose or suggest a hooking program residing at the location of said system call. In the present application, a hooking routine is located at the memory location designated for a system call (e.g., the memory location designated on the interrupt vector table). Grimm provides that "[i]nstead [of loading a software component for execution] the original software component is loaded and parsed as indicated in a block 12." Grimm doe not disclose or suggest that the loading and parsing are performed by a hooking routine located at the memory location designated for a system call.

Applicants respectfully contend that claims 1, 8, and 14, as originally filed are further allowable because they includes another feature that is neither disclosed nor suggested by Grimm or any other references cited in the Office Action, either individually or in combination, namely, "determine a data flow or process requested by said call." In the present application, when a system call is made, the hooking routine executes to monitor and display the operation of the computer system (see specification page 10, lines 1-8). The hooking routines generate an icon or other graphical representation of the current operation to be performed by the original routine (i.e., the routine called by the system call). The office action suggests that Grimm discloses this feature at Col. 4, lines 23-27, however Applicants respectfully disagree. The cited potion of Grimm provides that an introspection service 13 is provided when software component 11 as originally created needs to be loaded for execution by a computer. This passage does not disclose or suggest that the method of Grimm determines a data flow or process requested by said call. Grimm does provide that "[i]ntrospection service 13 determines abstractions or object types that are supported by software component as well as operations on these abstractions" (col. 5, lines 7-9). As explained in the present application, data flow or operations are monitored at a system call level. This allows the present invention to track an individual byte of information to monitor and display the operation of the computer without flooding the user with excessive information. Grimm does not provide data flow information to the user, but rather analyzes abstractions of a software component directed at determining security policy measures that might apply to the software component.

Applicants respectfully contend that claims 1, 8, and 14, as originally filed, are further allowable because they includes another feature that is neither disclosed nor suggested by Grimm or any other references cited in the Office Action, either individually or in combination, namely, "determine another data flow or process for data related to that of said call." The present invention provides for associating a current system call operation with another system call operation by matching file names or memory locations, for example. This step is important to creating a meaningful process flow to track a data flow or process. Grimm does not disclose or suggest stringing together related system call operations to track data flow or processes. The office action suggests that this feature is provided at col. 4, line 65 to col. 5, line 2 and at col. 6, lines 17-20. However, the cited text addresses the interception and parsing of a software

call.

Applicants respectfully contend that Claims 3 and 9 are allowable for the further reason that it includes another feature that is neither disclosed nor suggested by Grimm or any other reference cited in the office action either individually or in combination, namely "said information flow diagram illustrates locations of said data at stages of a processing activity." The present invention provides an embodiment in which the flow of data is captured and the location of the data at stages of processing is illustrated. This allows a user to quickly see where data is being transferred to, and therefore, whether data is being manipulated in an undesirable way. Grimm does not disclose or suggest illustrating locations of data during processing.

Applicants respectfully contend that Claims 4 and 10 are allowable for the further reason that it includes another feature that is neither disclosed nor suggested by Grimm or any other reference cited in the office action either individually or in combination, namely "said system call is selected from the set of: open file, copy file to memory, copy memory to register, mathematical functions, write to file, and network or communication functions." Grimm does not disclose or suggest a hook routine executing in response to any of the claimed system calls. The office action appears to suggest that this feature is disclosed by the statement in Grimm "Based upon information determined by introspection service 13, a security policy service 15 instructs an interposition service 17, which is also included in the present invention, how to modify the original software component to adhere to the security policies of the site." Applicants respectfully contend that modification of incoming software by adding access checks, protection domain transfers, and auditing does not disclose or suggest that a hook routine executes in response to one of the claim system calls.

Applicants respectfully contend that Claims 5 and 11 are allowable for the further reason that it includes another feature that is neither disclosed nor suggested by Grimm or any other reference cited in the office action either individually or in combination, namely "said system call is a software interrupt of an operating system." Grimm does not disclose or suggest a system call that is a system interrupt of the operating system. As with claim 4, the office action seems to suggest that modification of incoming software by adding access checks, protection domain transfers, and auditing discloses or suggests that the system call is a software interrupt of an operating system. Applicants respectfully disagree.

Applicants respectfully contend that Claims 6 and 12 are allowable for the further reason that it includes another feature that is neither disclosed nor suggested by Grimm or any other reference cited in the office action either individually or in combination, namely "said system call causes a processor to stop its current activity and execute said hook routine." Grimm does not disclose or suggest a system call that causes a processor to stop its current activity and execute said hook routine. As with claim 4, the office action seems to suggest that modification of incoming software by adding access checks, protection domain transfers, and auditing does not

disclose or suggest that the system call causes a processor to stop its current activity and execute said hook routine. Applicants respectfully disagree.

Conclusion

In view of the forgoing amendments and remarks, Applicants respectfully contend that claims 1-14 are in condition for allowance. Accordingly, Applicants respectfully request entry of the foregoing amendments, examination and allowance of the claims, and issuance of letters patent for this invention.

Sincerely,

Steven E. Bach
Reg. No. 46,530

US 106900160AP1

Creation date: 03-08-07
Indexing Officer: SMANH - SUZANE MANH
Team: ZZZFEP
Dossier: 10690016

Legal Date: 03-02-07

No.	Doccode	Number of pages
1	A...	1
2	SPEC	1
3	CLM	4
4	REM	4
5	SPEC	16
6	REM	16

Total number of pages: 42

Remarks:

Order of re-scan issued on .....